

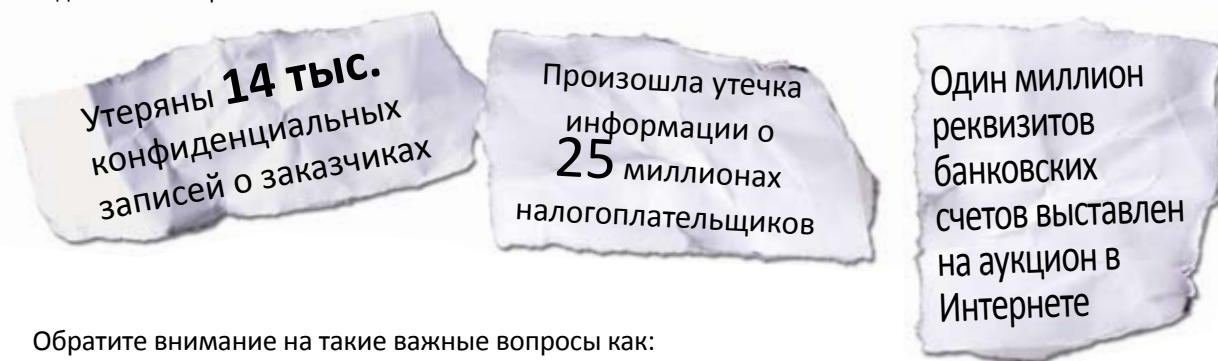
Уважаемый г-н/г-жа!

Представьте, если бы на этом CD находились данные о Ваших клиентах, а диск попал бы в руки Вашего главного конкурента?

К счастью, это не так. Диск чист и на нем ничего нет.

Потеря жизненно важной конфиденциальной информации – серьезная угроза для бизнеса. Это может быть список самых крупных клиентов, сведения о текущем проекте, либо закрытая информация о финансовой деятельности – все эти данные представляют огромную ценность для компании. Потеря или кража данных может привести к тяжелым последствиям: потенциальным штрафам, потере клиентов и бизнеса или ущербу для репутации.

В большинстве компаний недовольные сотрудники могут легко украсть данные. Последние исследования аналитиков Forrester Research показывают, что источником **80 %** угроз для информационной безопасности компаний являются действия сотрудников. Вот только некоторые известные случаи нарушения безопасности и кражи данных, о которых недавно писала пресса.



Обратите внимание на такие важные вопросы как:

1. Можете ли Вы ввести ограничения на то, кто, когда и где получает доступ к приложениям, базам данных и информации?
2. Насколько легко пользователям выгружать данные и уносить их за пределы компании?
3. Вы уверены в том, что информация, необходимая для контролирующих органов и аудита, защищена?

В нестабильной экономической ситуации, когда сохранять рабочие места становится все сложнее, а сокращения штатов происходят все чаще, еще более важно предпринимать меры для того, чтобы данные компании не покидали ее вместе с сотрудниками. Вы как руководитель высшего звена должны делать все возможное, чтобы предотвращать внутренние угрозы для безопасности данных.

С помощью решений Oracle можно предотвратить несанкционированный доступ к данным.

- **Oracle Access Manager** обеспечивает простой метод регистрации и информационные сервисы для безопасного доступа к важным Web-ресурсам и приложениям, а также является основой для управления регистрационными данными пользователей, паролями и политиками авторизации.
- **Oracle Information Rights Management** использует механизм шифрования документов и электронных писем, а также цифровую подпись для защиты от действий злоумышленников.
- Защиту данных компании и соблюдение нормативных требований можно контролировать с помощью опции **Oracle Database Vault**.

Не рискуйте. Узнайте о том, как защитить важные данные. Вы можете посетить страницу www.safe-data.eu/ru, чтобы ознакомиться с набором средств для обеспечения безопасности. Также вы можете обратиться за дополнительной информацией в Центр Oracle по работе с клиентами. Пусть данные остаются там, где им следует находиться – в Ваших руках.

С уважением,
Центр Oracle по работе с клиентами

тел. для России: +7 (495) 981-47-80,
тел. для Казахстана: 8 (800) 080-09-87,
e-mail: oracle_ru@oracle.com

